

Statement of Melissa Smislova, Acting Director
Homeland Infrastructure Threat and Risk Analysis Center
US Department of Homeland Security
before the
House Committee on Homeland Security Subcommittee on
Intelligence, Information Sharing, and Terrorism Risk Assessment
“Terrorism Risk Assessment at the Department of Homeland
Security”

November 17, 2005

Introduction

Good afternoon, Mr. Chairman and distinguished Members of this Committee. I am here to speak with you about the role of the Office of Intelligence & Analysis in the development of DHS risk assessments.

As Secretary Chertoff has reinforced throughout his tenure, DHS has adopted a risk-based approach in both our operations and our philosophy. There is no question that intelligence is a key component of risk analysis. For this reason, the Office of Intelligence & Analysis and the Office of Infrastructure Protection established the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) to institutionalize strategic risk assessments and produce tailored threat documents in support of the protection of national critical infrastructure and key resources (CI/KR).

Homeland Infrastructure and Risk Analysis Center

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) reports to both the Office of Intelligence Analysis (OI & A) and the Office of Infrastructure Protection (OIP). It brings together members of the Intelligence Community under OI & A and infrastructure specialists from the OIP as well as experts from the National Communications System and the National Cyber Security Division, among others, to produce strategic-level risk assessments. Under this dual structure, priority of infrastructure work requirements come from the Assistant Secretary for Infrastructure Protection, Mr. Robert Stephan, while approval for all intelligence derived production remains with the Assistant Secretary for Intelligence and Analysis, Mr. Charlie Allen.

The HITRAC mission represents a unique capability within the U.S. Government. HITRAC threat analysts have access to traditional intelligence community reporting and data as well as to DHS component-specific intelligence and information reporting (for example, information gathered at the ports of entry and transportation centers by DHS component members). HITRAC infrastructure protection sector specialists, who possess private sector expertise and sector specific incident data, identify sector-specific vulnerabilities and consequences of attack. HITRAC analysts then integrate all available information to produce strategic-level risk assessments for Federal, State and local authorities and the private sector.

HITRAC crafts products that make intelligence information more relevant to infrastructure owners and operators by framing our analysis in the context and unique operating environment of all seventeen CI/KR sectors. HITRAC receives information about the critical infrastructure through our Information Sharing and Analysis Centers and through contacts with private and public infrastructure owners that have been established by the OIP and throughout the Preparedness Directorate. In addition we are able to refine national intelligence community collection requirements though working with OI&A.

In addition, HITRAC produces threat products for infrastructure owners and operators to use in their own risk calculations and for DHS, state and local entities, and other Federal entities to use

in their own planning and operations. DHS defines risk as a determination of weighing the factors of threat, vulnerability and consequence. While inherently the most subjective component of the risk equation, threat of enemy attack is derived from study of enemy intent and capability. Intent of this adversary is assessed after study of all available information about what they want to accomplish by attacking the United States. We work with our partners in the intelligence community to understand as much as we are able about the terrorists' goals, plans, and desires. We match what we know about the intentions of the adversary with information we have about what the enemy is capable of accomplishing. For this part of the equation we rely both on what we see the enemy discussing, recruiting and training for as well as lessons learned from overseas attacks. We work all the pieces of the information puzzle. HITRACs unique partnering with Infrastructure Protection specialists that are not professional intelligence officers allows us a different view of the data than our IC colleagues.

Threat Products Supporting the National Infrastructure Protection Plan

One example of the integration of threat analysis with DHS risk assessment efforts is in the HITRAC production plan to support the National Infrastructure Protection Plan. Directed by Homeland Security Presidential Directive 7 (HSPD-7), the National Infrastructure Protection Plan (NIPP) is a unified national plan for the consolidation of critical infrastructure protection activities. The NIPP is a collaborative effort between the private sector, State, local, territorial and tribal entities and all relevant departments and agencies of the Federal government.

The cornerstone of the NIPP is a risk management framework that combines threat, vulnerability, and consequence information to produce a comprehensive, systematic, and informed assessment of national or sector risk that drives our protection efforts in the CI/KR sectors. This framework applies to the general threat environment as well as specific threats or incident situations.

HITRAC's production plan supports the NIPP. The NIPP promises sector specific threat information to each sector following its finalization. Our analytic products are designed to provide threat information to the private and public infrastructure owners and operators. In particular we are producing:

- **Sector Assessments** for each CI/KR sector. HITRAC through the OI & A and in coordination with TSA and USCG intelligence entities will produce several sub-sector assessments due to the broad characteristics of some sectors (for example, HITRAC will produce sub-sector assessments for aviation and mass transit which are sub-sectors of the broader transportation sector). HITRAC leverages the expertise of several sector specific agencies, including the Transportation Security Administration, as well as our colleagues in the intelligence community to support our efforts. These products, written at multiple classification levels, provide DHS a vehicle to deliver long-term strategic assessments of sector risks by detailing HITRAC analysis of the intentions and capabilities of known terrorists and integrating relevant threat information with the unique vulnerabilities and consequence of each sector.
- HITRAC is also producing **Common Threat Themes** in support of the NIPP and other DHS and Federal risk assessments. These threat scenarios are descriptions of potential attack

methods based on known or desired terrorist capabilities. These scenarios, which will be updated as needed, are detailed vignettes of the methods terrorist might use to attack the US infrastructure and are derived from the study of terrorist intentions and capabilities. These scenarios are intended to inform vulnerability and consequence analysis while ensuring that a given risk analysis has taken into account the minimum set of potential attack vectors and the associated vulnerabilities and consequences.

These threat themes are used as the foundations to design and build the threat scenarios used by the Office of Domestic Preparedness. The scenarios used for ODP exercises are lengthy depictions of how a notional terrorist attack might unfold and they are drafted to test prevention and response capabilities. HITRAC's threat themes are specific descriptions of ways the enemy can attack and are for use by private and public infrastructure owners and state and local governments to develop their own risk assessments. For example, they describe in detail what we know about how the adversary can employ a vehicle borne improvised explosive device.

Conclusion

The Federal government and private sector owners and operators need intelligence-based risk assessments to best protect against and respond to potential terrorist attacks. DHS established HITRAC to provide integrated strategic risk assessments and tailored threat products in support of the protection of critical infrastructure and key resources throughout the nation. This is a very challenging mission, but with your support, we will succeed.

Thank you.